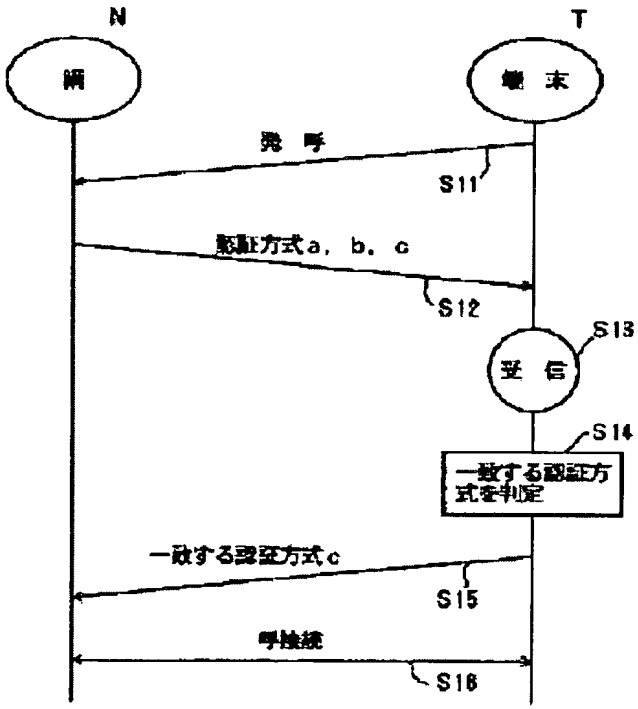
VERIFICATION CONTROL SYSTEM

Patent number:	JP6261033
Publication date:	1994-09-16
Inventor:	SHIMADA MASAKI; others: 02
Applicant:	NIPPON TELEGR & TELEPH CORP
Classification:	
- international:	H04L9/00; H04L9/10; H04L9/12; G09C1/00
- european:	
Application number:	JP19930046984 19930308
Priority number(s):	

Abstract of **JP6261033**

PURPOSE:To allow a network to simply decide the verification system without notifying the verification system of a terminal equipment by providing plural verification means to the network, selecting one of them and informing the selected system to the terminal equipment and allowing the terminal equipment to select one of the executionable verification systems when it is included in the notice and giving a reply to the network.

CONSTITUTION:A terminal equipment T makes a call to a network N. Upon the receipt of a connection request from the terminal equipment T, the network N sends information about verification systems a-c possessed by the network N to the terminal equipment T. The terminal equipment T discriminates whether or not a system coincident with the verification system of its own is in existence among the verification systems noticed from the network N. When there is any coincident verification system, the terminal equipment T informs the verification system to the network N. Since the verification system noticed from the terminal equipment T is coincident with that informed from the network N, the network N verifies the terminal equipment T and the network N and the terminal equipment T are interconnected.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平6－261033

(43)公開日　平成６年(1994)９月16日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｇ０９Ｃ	1/00		8837－5L		
			7117－5K	Ｈ０４Ｌ　9/ 00　Ｚ	

審査請求　未請求　請求項の数１　ＯＬ　（全 ７ 頁）

(21)出願番号　特願平5－46984

(22)出願日　平成５年(1993)３月８日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号

(72)発明者　嶋田　勝紀
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　前田　潤二
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　舟川　公敏
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　伊東　忠彦

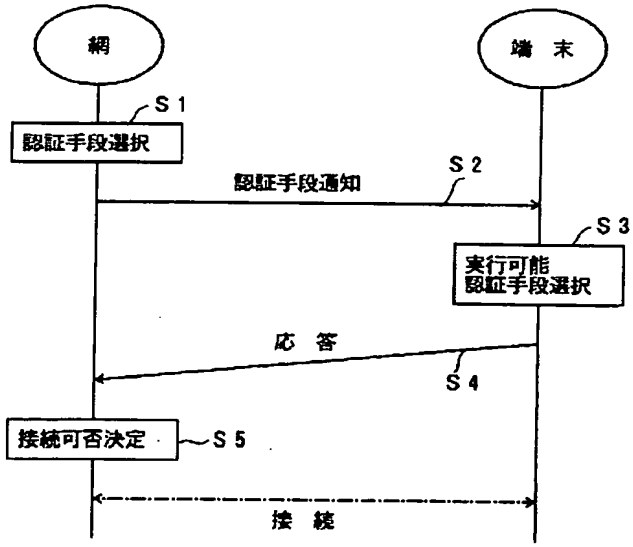
(54)【発明の名称】　認証制御方式

(57)【要約】

【目的】　本発明の目的は、網が端末のもつ認証方式を意識することなしに、簡易に認証方式を決定することができる認証制御方式を提供することである。

【構成】　本発明は、網が端末を認証するための複数の認証手段を有し、認証手段から少なくとも１つの認証手段を選択して（ステップ１）、端末に通知し（ステップ２）、端末が網からの該通知の中に実行可能な認証手段が含まれる場合に、認証手段のうち１つを選択して（ステップ３）網に応答し（ステップ４）、網が端末間の認証手段が同一であるか判断し（ステップ５）、等しければ網と端末間を接続可能とする（ステップ６）。

本発明の原理説明図



1

【特許請求の範囲】

【請求項１】　端末との接続時に該端末の認証を行う網と、認証手段を具備する端末とを含む通信システムにおける認証制御方式において、

該網は端末を認証するための複数の認証手段を有し、該認証手段から少なくとも１つの認証手段を選択して、該端末に通知し、

該端末は該網からの該通知の中に実行可能な認証手段が含まれる場合に、該認証手段のうち１つを選択して該網に応答し、

該網は該端末間の該認証手段が同一であるか判断し、等しければ該網と該端末間を接続可能であると認証することを特徴とする認証制御方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は認証制御方式に係り、特に通信におけるセキュリティの保護のために網側から端末の正当性をチェックするための認証を必要とする通信システムの認証制御方式に関する。

【０００２】

【従来の技術】従来の第１の認証を行う方式を説明する。移動通信方式に必要な認証を行う方式として、文献“花岡、尾上、上林、「ディジタル移動通信網における認証方式」電子情報通信学会、秋期全国大会、pp. ２－２３２、１９９０年”がある。この方法は、認証を行うユーザ間で共有される秘密の暗号鍵Ｋ１を用いて、認証起動側のユーザから適当な平文と鍵Ｋ１を用いた暗号文Ｃを送信し、被認証側ユーザは受信した平文から暗号鍵Ｋ１を用いて暗号文Ｃ’を生成し、認証起動側ユーザに返送する。ここで、暗号文ＣとＣ’が等しければ認証ができたことになる。

【０００３】次に従来の第２の認証を行う方式を説明する。図６は従来の第２の認証方式の一例を示すブロック図である。同図において、網Ｎ１は認証方式ａを有し、網Ｎ２は認証方式ｂを有する。また、端末Ｔ１は認証方式のａを有し、端末Ｔ２は認証方式ｂを有する。

【０００４】このとき、同一の認証方式を具備する端末Ｔ１と網Ｎ１との間では、

①端末Ｔ１が網Ｎ１に接続を要求すると、

②網Ｎ１が認証鍵により決定される認証情報を端末Ｔ１に送信し、端末Ｔ１に認証を要求する。

③端末Ｔ１は、網Ｎ１からの認証情報に対応する認証応答情報を含む応答を網Ｎ１に応答する。

④網Ｎ１が認証応答情報の正当性を確認した後に、端末Ｔ１の接続を確認する。

【０００５】一方、同図において、点線で示される関係のように、網Ｎと端末Ｔの具備する認証方式が異なる場合には、網Ｎと端末Ｔ間の認証は許容されない。従って、異なる認証では接続されないためにセキュリティーが守られる。

2

【０００６】ここで、認証方式ａを具備する端末Ｔ１と、認証方式ｂを採用する網Ｎ２があるとする。この端末Ｔ１と網Ｎ２間の接続を可能とするためには、網Ｎ２と端末Ｔ１の何れかが複数の認証方式を具備する必要がある。例えば、網Ｎ２が端末Ｔ１の正当性を認証により確認するためには、網Ｎ２の指定した認証方式に端末Ｔ１が従うものとし、網Ｎ２に指定された認証方式を端末Ｔ１が備えていれば認証が成立する。

【０００７】そのため、異なる認証方式を採用している複数の通信システムにおいて、同一の端末が利用可能とするためには、相互接続を可能とするシステム間で互いの認証方式を具備しなければならない。

【０００８】図７は従来の第２の認証方式における網のメモリを示す。同図に示すように網は各端末毎に具備している認証方式１１をメモリ１０内に記憶する。同図の例では、端末Ｔ１が有する認証方式はａ、端末Ｔ２が有する認証方式はｂ、端末Ｔ３が有する認証方式はａというように、認証方式を各端末毎に具備する。例えば、網Ｎが端末Ｔに対してメモリ１０に記憶してあるメモリ内情報１１（認証方式）よりｂを通知して、端末からｂの認証方式が通知されれば網Ｎは端末Ｔを認証する。

【０００９】また、網との接続を希望する端末が網の認証方式を具備する方式もある。図８は従来の第２の認証方式における端末が有する認証方式を示す。同図において、端末は接続を希望する網の認証方式を具備するものとする。

【００１０】同図の例では、この端末の端末内メモリ２０が有するメモリ内情報２１（認証方式）は、方式ａ，方式ｂ，方式ｃ等である。ここで、網Ｎから方式ａが通知された場合には認証され、網Ｎから認証方式としてｄが通知された場合には、この端末には、認証方式ｄが具備されていないので、認証されない。

【００１１】

【発明が解決しようとする課題】しかしながら、上記第１の従来の方式では、暗号鍵等を予め設定して認証側及び被認証側でそれぞれ同じ暗号鍵を保持するため、鍵の変更時に、認証側で暗号鍵を変更しても被認証側で変更が終了しておらず、鍵に矛盾が発生することがある。この場合には、暗号文が認証側と被認証側で一致することがないために認証が成功しない。また、鍵を第３者により悪用されることも考えられる。

【００１２】また、上記第２の方式では、網が認証すべき端末毎の認証方式を記憶するためには、端末数に見合う記憶領域を必要とし、端末で複数の認証方式を持つ方式では、後で網の利用を要求するシステムが増加した場合に認証方式の追加が困難である。

【００１３】本発明は上記の点に鑑みなされたもので、上記従来の問題点を解決し、網が端末のもつ認証方式を意識することなしに、網と端末の間での交渉により簡易に認証方式を決定することができる認証制御方式を提供

することを目的とする。

【００１４】

【課題を解決するための手段】図１は本発明の原理説明図である。

【００１５】端末との接続時に該端末の認証を行う網と、認証手段を具備する端末とを含む通信システムにおける認証制御方式において、網は端末を認証するための複数の認証手段を有し、認証手段から少なくとも１つの認証手段を選択して（ステップ１）、端末に通知し（ステップ２）、端末は網からの通知の中に実行可能な認証手段が含まれる場合に、認証手段のうち１つを選択して（ステップ３）網に応答し（ステップ４）、網は端末間の認証手段が同一であるか判断し（ステップ５）、等しければ網と端末間を接続可能であると認証する（ステップ６）。

【００１６】

【作用】本発明は、網に認証方式を複数持たせ、端末は網の持つ認証方式のうち何れかを持つことにより、網が端末の持つ認証方式を意識せずに、認証方式を端末に通知する。端末は網からの１つの認証方式に限定されることなく、自端末が有している認証方式が網から通知された認証方式に含まれていれば、網に接続要求を行うことができる。一方、端末が保持していない認証方式で網にアクセスしても網は接続を許可しないため、通信のセキュリティを保つことができる。

【００１７】

【実施例】以下、図面により本発明の実施例を説明する。

【００１８】図２は本発明の第１の実施例のブロック構成図である。同図において、網Ｎは複数の認証方式ａ，ｂ，ｃを有し、端末Ｔは認証方式ｃ，ｄを有する。このような関連において、網Ｎと端末Ｔの接続の認証について説明する。

【００１９】図３は本発明の第１の実施例の処理のタイミングチャートである。

【００２０】ステップ１１）まず、最初に端末Ｔが網Ｎに対して発呼する（または、網Ｎから着呼）。

【００２１】ステップ１２）網Ｎは端末Ｔからの接続要求を受信すると、端末Ｔに対して、網Ｎが有する認証方式ａ，ｂ，ｃを送出する。

【００２２】ステップ１３）端末Ｔは網Ｎからの認証方式ａ，ｂ，ｃを受信する。

【００２３】ステップ１４）端末Ｔは網Ｎからの認証方式のうち、自端末に有する認証方式と一致する方式があるかを判定する。

【００２４】ステップ１５）ステップ４において、一致する認証方式が有る場合には、その認証方式を網Ｎに送信する。この例の場合には、認証方式ｃが一致しているので、網Ｎに認証方式ｃを送出する。

【００２５】ステップ１６）これにより、網Ｎでは認証方式ｃが一致しているために端末Ｔを認証し、網Ｎと端末Ｔが接続される。

【００２６】また、端末Ｔが認証方式ｄ，ｃを有している場合には、網Ｎから通知した認証方式には認証方式ｄ，ｅは含まれていないため、認証されない。

【００２７】次に、本発明の第２の実施例として、予め認証強度により認証方式を決定する場合について説明する。本実施例では、認証強度に対応する認証方式を用いる方式について説明する。

【００２８】図４は本発明の第２の実施例の認証方式の設定を説明するための図である。同図において、網Ｎまたは端末Ｔの認証設定部４０と、網Ｎから端末Ｔ、または端末Ｔから網Ｎに対しての通信を行うためのインターフェース部５０から構成される。認証設定部４０は、バッファメモリ４１、強度比較部４２、認証方式テーブル作成部４３、認証方式テーブル４４により構成される。

【００２９】本実施例における認証方式に設定は、まず、網Ｎまたは端末Ｔの認証設定部４０に重要度に基づいた認証強度が入力され、一旦入力された認証強度をバッファメモリ４１に蓄える。次に、強度比較部４２において、先に入力された認証強度との比較を行い、強度が大きい順にバッファメモリ４１にソートしておく。認証方式テーブル作成部４３は、最高強度のものを強度１とし、認証方式ａとする。さらに、２番目の強度のものを強度２とし、認証方式ｂとする。同様に３番目の強度のものを強度３とし、認証方式ｃとする。このように強度に対応する認証方式を認証方式テーブル４４に設定する。

【００３０】例えば、網Ｎはインターフェース部５０により端末Ｎから接続要求があった場合に、このように認証方式テーブル４４に設定された認証方式を読みだして端末Ｔに通知する。上記認証方式の設定は、網Ｎ側、端末Ｔ側共に予め設定されるものとする。

【００３１】図５は本発明の第２の実施例の網及び端末の認証方式を示す。網Ｎには強度１を認証方式ａ、強度２を認証方式ｂ、強度３を認証方式ｃとして設定されている。また、端末Ｔは、強度１を認証方式ａ、強度３を認証方式ｃとした２つの認証方式を有している。

【００３２】図５における認証について説明する。認証を行うためのシーケンスは図３に示すシーケンスと同様である。以下の説明において、網Ｎを移動通信における無線回線制御局とし、端末Ｔを移動局として説明する。

【００３３】まず、移動局から無線回線制御局に発呼することにより呼接続要求を行う。接続要求を受信した無線回線制御局は、自局が有する認証方式ａ，ｂ，ｃを移動局に通知する。

【００３４】移動局は、無線回線制御局から通知された認証方式ａ，ｂ，ｃのうち自端末が有する認証方式がその中に含まれているかを判断する。図５の例では、認証方式ａ，ｃが含まれているので、その認証方式ａ，ｂを

5

無線回線制御局に送出する。無線回線制御局は、移動局からの通知を受け取ると、同じ認証方式を持つ移動局を認証し、移動局間の呼接続を行う。

【００３５】また、移動局が強度２の認証方式ｂ、強度４の認証方式ｄを有している場合には、移動局は無線回線制御局から通知された認証方式に含まれる認証方式を持たないため、無線回線制御局からの認証は行われない。従って、無線回線制御局間の呼接続は行われない。

【００３６】なお、本発明は、網及び端末の両方に複数の認証方式を保持しているが、網側から端末に通知される認証方式が複数であればよく、端末側が常時、複数の認証方式を保持する必要はない。

【００３７】なお、本発明は本発明の主旨を逸脱しない範囲で網から端末を認証できる方式であれば、上記実施例に限定されることなく種々変更が可能である。

【００３８】

【発明の効果】上述のように本発明の認証制御方式によれば、網が端末の持つ認証方式を意識せずに、認証方式を端末に通知し、端末は網のもつ認証方式のうち何れかを有していれば、網は端末を認証することができる。また、一方、端末側で網から通知された認証方式を持っていない場合には、認証されないため、通信におけるセキュリティを保つことができる。

【００３９】また、重要度等、網と端末との関連に応じて認証方式を互いに設定しておくこともできるため、関連重要度の高い順に接続を行うことも可能である。

【図面の簡単な説明】

【図１】本発明の原理説明図である。

6

＊【図２】本発明の第１の実施例のブロック構成図である。

【図３】本発明の第１の実施例の処理のシーケンスチャートである。

【図４】本発明の第２の実施例の認証方式の設定を説明するための図である。

【図５】本発明の第２の実施例の網及び端末の認証方式を示す図である。

【図６】従来の第２の認証方式の一例を示すブロック図である。

【図７】従来の第２の認証方式における網のメモリを示す図である。

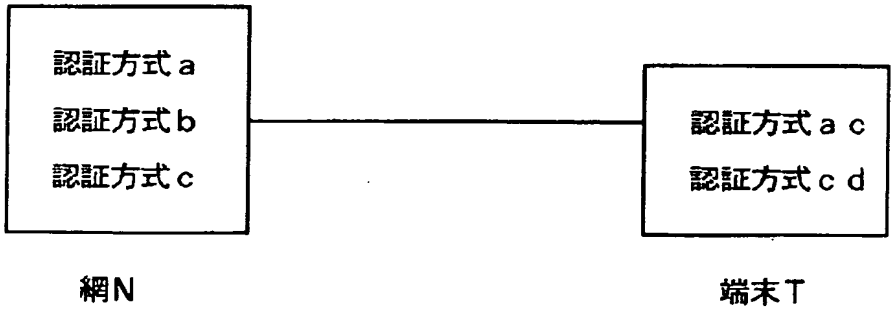
【図８】従来の第２の認証方式における端末が有する認証方式を示す図である。

【符号の説明】

Ｎ，Ｎ１，Ｎ２　網
Ｔ　端末
１０　メモリ
１１　メモリ内情報（認証方式）
２０　端末メモリ
２１　端末メモリ内情報（認証方式）
４０　認証設定部
４１　バッファメモリ
４２　強度比較部
４３　認証方式テーブル作成部
４４　認証方式テーブル
５０　インターフェース部

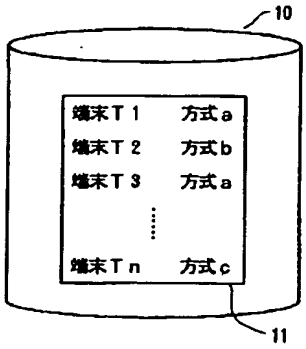
【図２】

本発明の第１の実施例のブロック構成図



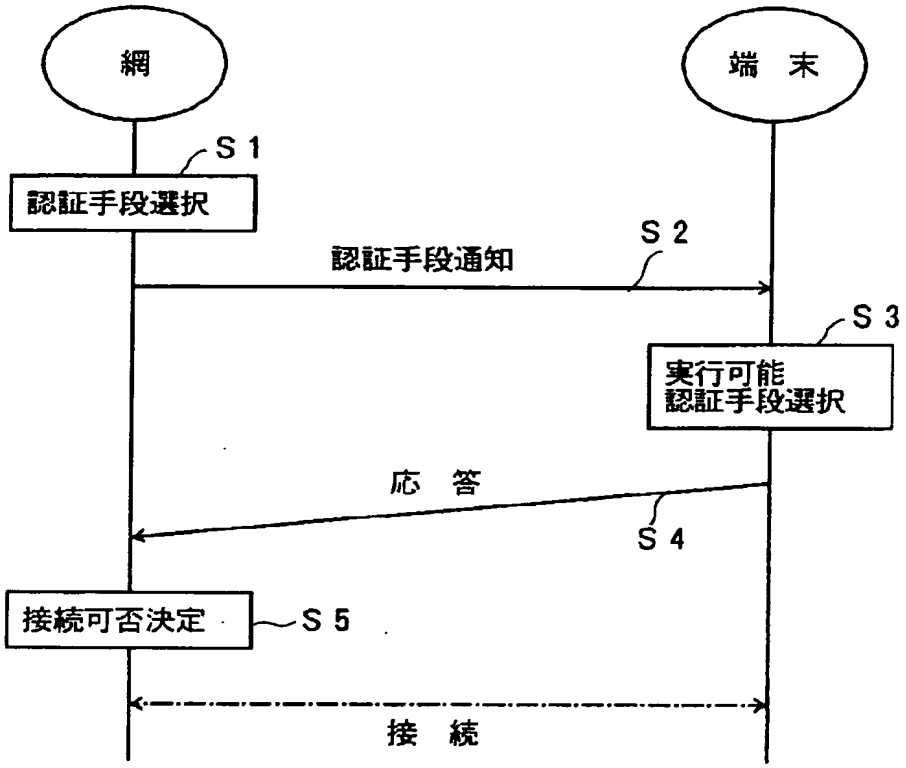
【図７】

従来の第２の認証方式における網のメモリを示す図



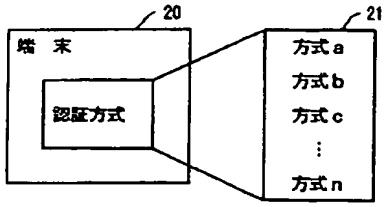
【図１】

本発明の原理説明図



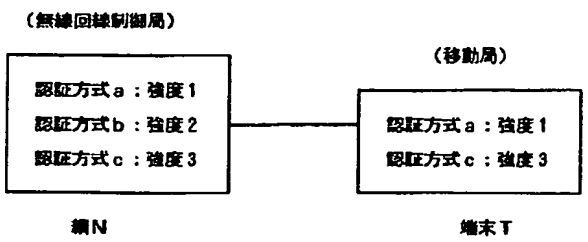
【図８】

従来の第２の認証方式における端末が有する認証方式を示す図



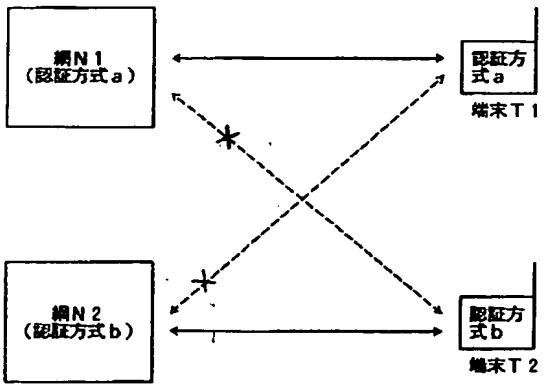
【図５】

本発明の第２の実施例の網及び端末の認証方式を示す図



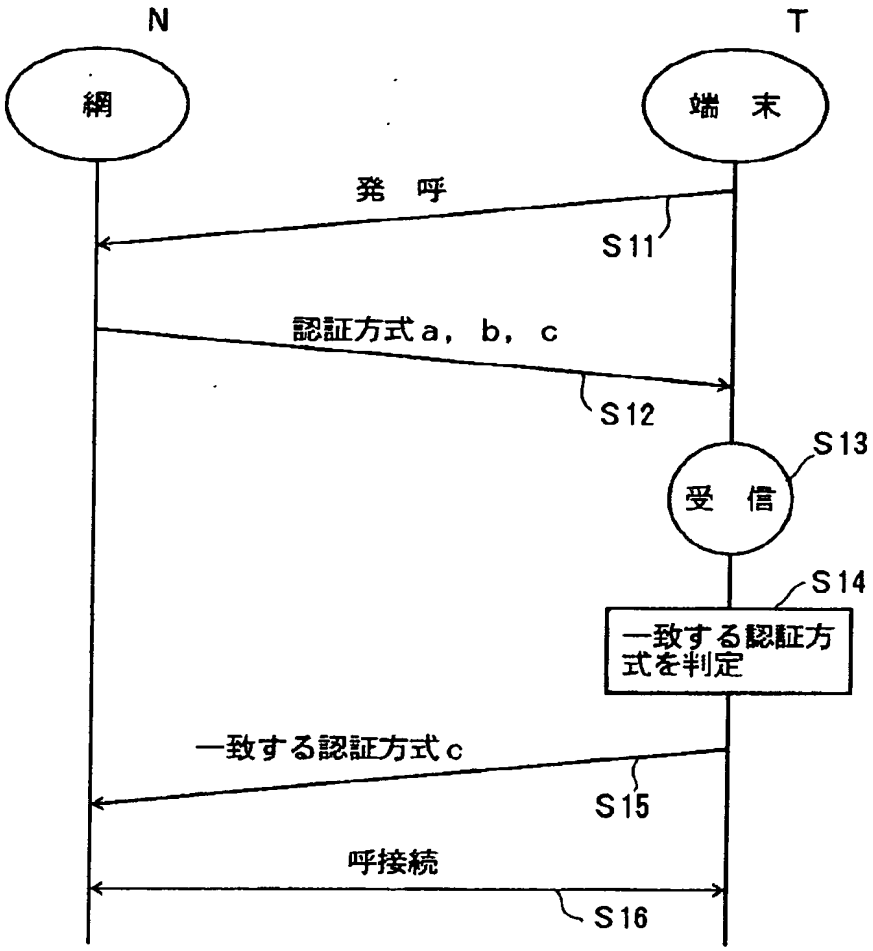
【図６】

従来の第２の認証方式の一例を示すブロック図



【図３】

本発明の第１の実施例の処理のシーケンスチャート



【図４】

本発明の第２の実施例の認証方式設定を説明するための図